INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Implementation of DOD Public Key Infrastructure Policy and Procedures

B. DATE Report Downloaded From the Internet: 01/10/02

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 01/10/02**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

Audit Report

IMPLEMENTATION OF DOD PUBLIC KEY INFRASTRUCTURE POLICY AND PROCEDURES

Report No. D-2002-030 December 28, 2001

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this audit report, visit the Inspector General, DoD, Home Page at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ASD(C^3I)	Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
CAC	Common Access Card
CCA	Clinger-Cohen Act
CIO	Chief Information Officer
DEERS	Defense Enrollment Eligibility Registration System
IA	Information Assurance
IT	Information Technology
PKE	Public Key-Enabled
PKI	Public Key Infrastructure
PMO	Program Management Office
RAPIDS	Real-time Automated Personnel Identification System

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

December 28, 2001

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)

SUBJECT: Audit Report on the Implementation of DoD Public Key Infrastructure Policy and Procedures (Report No. D-2002-030)

We are providing this audit report for your information and use. We conducted the audit as part of our ongoing efforts to review information assurance within DoD. We considered management comments on a draft of this report when preparing the final report.

The comments of the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required.

We appreciate the courtesies extended to the audit staff. Questions on this report should be directed to Ms. Wanda A. Scott at (703) 604-9049 (DSN 664-9049) (wascott@dodig.osd.mil) or Ms. Dianna J. Pearson at (703) 604-9063 (DSN 664-9063) (djpearson@dodig.osd.mil). See Appendix E for the report distribution. The audit team members are listed inside the back cover.

David K. Steensma

David K. Steensma
Acting Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2002-030 **December 28, 2001**
(Project No. D2001AS-0008)

Implementation of DoD Public Key Infrastructure Policy and Procedures

Executive Summary

Introduction. Federal agencies, including DoD, are increasingly using the World Wide Web and other Internet-based applications to provide on-line public access to information and services as well as to improve internal business operations. However, the potential for improvements in service delivery and productivity due to electronic and Internet-based applications come with many of the security risks faced by existing systems as well as new risks. To achieve information superiority in a highly interconnected, shared-risk environment, DoD Information Assurance capabilities must address the pervasiveness of information as a vital aspect of warfighting and business operations. The Defense-in-Depth strategy is the technical strategy that underlies DoD information assurance in which layers of defense are used to achieve security objectives. One element of the Defense-in-Depth strategy is the use of a common, integrated, interoperable DoD Public Key Infrastructure to enable security services at multiple levels of assurance. As of October 2000, the funding allocation for the DoD Public Key Infrastructure for FYs 2001 through 2005 was about $712 million.

Objectives. The overall objective was to evaluate the implementation and management of Public Key Infrastructure within the DoD. Specifically, we evaluated the DoD oversight of Public Key Infrastructure, coordination of Public Key Infrastructure missions and pilot programs among the Services and DoD agencies, and compliance with the Clinger-Cohen Act. We did not review the management control program relating to the overall objective because DoD designated information assurance as a systemic management control weakness in the FY 2000 Annual Statement of Assurance.

Results. Although progress had been made in implementing Public Key Infrastructure, DoD had not managed the DoD Public Key Infrastructure Program as an enterprise-wide information technology investment. As a result, DoD will not be able to adequately assess cost, performance, and schedule risks to Public Key Infrastructure implementation and use those assessments to determine whether the Public Key Infrastructure Program is cost-effectively meeting security requirements and user needs. See the Finding section for details on the audit results.

Summary of Recommendations. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) develop and implement oversight and management criteria for the Public Key Infrastructure investment. We also recommend that the Director, Public Key Infrastructure Program, develop an Information Technology Investment Management Plan for the DoD Public Key Infrastructure Program that addresses performance measures for the Public Key Infrastructure, a risk management plan, and DoD acquisition policy.

Management Comments. The Director, Information Assurance, provided a consolidated response for the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) and the Director, DoD Public Key Infrastructure Program Management Office. Both offices fully concurred with the report finding and recommendations. Specifically, the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) agreed to develop and implement oversight and management criteria for the DoD Public Key Infrastructure investment in accordance with DoD Directive 5000.1, "The Defense Acquisition System." The Director, DoD Public Key Infrastructure Program Management Office, agreed to develop an information technology Investment Management Plan for the Public Key Infrastructure Program that, at a minimum, addresses performance measures, a comprehensive risk management plan, and application of DoD acquisition policy requirements. A discussion of the management comments is in the Finding section of the report and the complete text is in the Management Comments section.

Table of Contents

Introduction

Federal agencies, including DoD, are increasingly using the World Wide Web and other Internet-based applications to provide on-line public access to information and services as well as to improve internal business operations. However, the potential for improvements in service delivery and productivity because of electronic and Internet-based applications come with new security risks and with the security risks already faced by existing systems.

To achieve information superiority[1] in a highly interconnected, shared-risk environment, DoD Information Assurance (IA) capabilities must address the pervasiveness of information as a vital aspect of warfighting and business operations. The Defense-in-Depth strategy is the technical strategy that underlies DoD IA in which layers of defense are used to achieve security objectives. That strategy recognizes the diversity of technologies, solutions, adversaries, and vulnerabilities that pervade our information systems and infrastructures. The strategy also recognizes that no single element can independently provide adequate assurance and that layers of defense at varying strengths and assurance levels can be deployed to provide multiple roadblocks between sensitive information systems and those internal and external adversaries who would try to exploit them. One element of the Defense-in-Depth strategy is the use of a common, integrated, interoperable Public Key Infrastructure (PKI) to enable security services at multiple levels of assurance.

Background

Description of PKI. A PKI is a system of hardware, software, policies, and people that, when fully and properly implemented, can provide a suite of information security assurances that are important in protecting sensitive communications and transactions. Specifically, PKI refers to the framework and services that provide for generating, producing, distributing, controlling, revoking, recovering, and tracking public key certificates[2] and their corresponding private keys. For PKI, key-pairs are generated by or for each user. Each key-pair comprises two keys (very large numbers, typically 150 to 300 digits in length), which are mathematically linked in a very subtle way. For each key-pair, one is kept private and the other is made public. See Appendix B for a graphical example of how the key pairs for PKI can work.

[1]Information superiority is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

[2]A certificate is a digital representation of information that binds the user's identification with the user's public key in a trusted manner. At a minimum, this information (1) identifies the certification authority issuing it, (2) names or identifies its user, (3) contains the user's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.

Public Key technology is rapidly becoming the technology of choice to enable security services within systems. These security services include:

- identification, which is a process that an information system uses to recognize an entity; and authentication, which is a security measure that is designed to establish the validity of a transmission, message, or originator or a means of verifying an individual's authorization to receive specific categories of information;

- data integrity, which means that data are unchanged from their source and have not been accidentally or maliciously modified, altered, or destroyed;

- confidentiality, which means that the information is not disclosed to unauthorized persons, processes, or devices; and

- non-repudiation, which is the assurance that the sender of the data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so that neither individual can later deny having sent or received the data.

DoD PKI Program. In April 1999, the Assistant Secretary of Defense (Command, Control, Communication, and Intelligence) [ASD(C^3I)], assigned program management responsibility to the National Security Agency and assigned deputy program management responsibility to the Defense Information Systems Agency for the implementation of a PKI throughout DoD. In response, the National Security Agency and Defense Information Systems Agency established the DoD PKI Program Management Office (PMO) to ensure that the DoD PKI supports validated and endorsed Public Key-Enabled (PKE) systems and applications that meet the broad spectrum of DoD mission and business needs. As lead agencies for the DoD PKI Program, the National Security Agency and the Defense Information Systems Agency were responsible for coordinating PKI activities within DoD by defining and providing general implementation guidance. The PMO was responsible for identifying and coordinating DoD PKI requirements and addressing interoperability, compatibility, commonality, and standardization issues. In addition, the PMO was responsible for the development and publication of a comprehensive PKI architecture, for a PKI implementation and transition plan, and for resolution of programmatic issues. The DoD plans to use an open standards approach[3] based on commercial products and services, while still maintaining appropriate levels of security.

[3]The DoD PKI is based on the use of commercial standards to the maximum extent feasible. DoD will ensure that its specifications are consistent with emerging commercial and National Institute of Standards and Technology Federal standards and will track new and evolving Internet standards to ensure that the most viable commercial standards are fully leveraged.

PKI Funding. As of October 2000, the DoD PKI budget for DoD was about $712 million for FYs 2001 through 2005. The PMO oversees spending of the $712 million, but each DoD Component manages its own portion of the $712 million. Funding for the PMO was about $1.4 million. The table below shows the allocation of PKI funding within DoD.

DoD PKI FYs 2001-2005 Funding Allocation as of October 16, 2000

Component	Amount (millions)
National Security Agency*	$134.00
Defense Information Systems Agency*	72.90
Army	140.20
Navy	107.20
Air Force	132.20
Marine Corps	56.63
Defense Logistics Agency	25.00
Others	43.50
Total	**$711.63**

*Amounts do not include the $1.4 million for the PMO.

PKI Guidance. The Deputy Secretary of Defense and the ASD(C^3I) issued several policy memorandums, which affected the evolution of the DoD PKI Program. See Appendix C for a chronology and discussion of the policy memorandums relative to the DoD PKI Program. On August 12, 2000, the ASD(C^3I) issued policy memorandum, "Department of Defense (DoD) Public Key Infrastructure (PKI)," which updated DoD policies for the development and implementation of a DoD-wide PKI and aligned PKI activities and milestones with those of the DoD Common Access Card (CAC) Program. On November 10, 1999, the Deputy Secretary of Defense issued policy memorandum, "Smart Card Adoption and Implementation," which directed the implementation of standard DoD smart card technology as a DoD-wide CAC. The Deputy Secretary also designated the CAC as the primary token[4] platform for PKI certificates and directed that the CAC also operate as the standard identification card, building access card. The memorandum also mandated using the Defense Enrollment Eligibility Reporting System (DEERS)[5] infrastructure and the Real-time Automated Personnel Identification System (RAPIDS)[6] to issue and maintain the CAC. Additionally, the Deputy Secretary of Defense authorized the DoD Chief Information Officer to modify the PKI guidance to incorporate and accommodate use of the CAC.

[4]A token is a device (floppy disk, Common Access Card, or smart card) that is used to protect and transport the private keys of a user.

[5]Defense Enrollment Eligibility Reporting System (DEERS) is a database, which contains status information on Uniformed Services members, their families, and DoD civilians.

[6]Real-time Automated Personnel Identification System (RAPIDS) is an automated, ID Card System for military, retired, and their families.

PKI Implementation. DoD had revised the schedule for PKI implementation based on requirements of the PKI guidance. The current implementation schedule is shown below.

Implementation Schedule

Class 3[7] Registration Capability	December 2001
All DoD Personnel Issued Class 3 Certificates	October 2002
All DoD Email Must be Digitally Signed with a Class 3 Certificate	October 2002
Begin Issuing Class 4 Certificates	October 2002
Protection of Unclassified Mission Critical Systems Must Migrate from Class 3 to Class 4	December 2003

Objectives

The overall objective was to evaluate the implementation and management of PKI within the DoD. Specifically, we evaluated DoD oversight of PKI, coordination of PKI missions and pilot programs among the Services and DoD agencies, and compliance with the requirements of the Clinger-Cohen Act. We did not review the management control program relating to the overall objective because DoD designated information assurance as a systemic management control weakness in the FY 2000 Annual Statement of Assurance. See Appendix A for a discussion of the audit scope and methodology.

[7]The level of assurance of a public key certificate is the degree of confidence in the binding of the identity to the public keys and privileges. DoD has identified the following assurance levels: Class 3 is for applications handling medium value information in a low to medium risk environment; Class 4 is for applications handling medium to high value information in a minimally protected environment.

Status of the Implementation of the DoD Public Key Infrastructure Program

Although progress had been made in implementing PKI within DoD, the PKI PMO had not managed the DoD PKI Program as a DoD enterprise-wide information technology (IT) investment. This condition occurred because the PMO had not:

- developed a coordinated DoD-wide IT investment plan that identified performance measures and managed risks that could affect PKI implementation;
- considered the PKI Program to be subject to DoD acquisition policy, which requires a process to document and collectively manage cost, performance, and schedule parameters for a program investment; and
- complied with the DoD implementation of the Clinger-Cohen Act (CCA) for managing IT investments.

Additionally, the DoD Chief Information Officer (CIO) had not developed or implemented oversight and management criteria for evaluating the PKI Program because it was designated only as a special interest initiative program. As a result, DoD will not be able to adequately assess cost, performance, and schedule risks to PKI implementation and use those assessments to determine whether the PKI Program is cost-effectively meeting security requirements and user needs.

Progress In Implementing the DoD PKI Program

The PMO took action and made progress in implementing the PKI Program. Specifically, the PMO issued various management and operational documents, established working groups, provided periodic status briefs, and identified unfunded requirements.

Management and Operational Documents. The PMO ensures that the management and planning documents provided for the PKI Program reflect Federal PKI requirements. Those documents included the "Public Key Infrastructure Roadmap for Department of Defense," (PKI Roadmap), December 18, 2000; the "X.509 Certificate Policy for the United States Department of Defense" (X.509 Certificate Policy), November 13, 2000; and the "Public Key Infrastructure Implementation Plan for the Department of Defense" (PKI Implementation Plan), December 18, 2000, and are discussed below.

The **PKI Roadmap.** The PKI Roadmap established the overall plan for the DoD PKI Program that outlined the strategy and timelines for the availability of PKI capabilities. The PKI Roadmap also defined how the DoD PKI would evolve into its final target architecture. The PMO reviewed and updated the PKI Roadmap, as appropriate, to reflect changes in direction or strategy.

The X.509 Certificate Policy. The PMO issued the X.509 Certificate Policy, which established the unified policy for creating and managing a Certification Authority and its related components. The Certificate Policy also defined how certificates will be created and managed and used with PKE applications.

The PKI Implementation Plan. The PKI Implementation provided for the phased implementation of a DoD-wide PKI and helped to coordinate PKI across the Services and among DoD activities. The PKI Implementation Plan documents how to implement the PKI Program and establishes the foundation for collecting information on the status of PKI.

Working Groups. The PMO established several working groups to address major areas of the PKI Program. The PKI working groups included the Certificate Policy Management Working Group, the Technical Working Group, the Business Working Group, and the Tactical Working Group. The PMO established the working groups to serve as focal points for DoD activities, to present issues and concerns on the DoD PKI Program implementation, and to resolve those issues and concerns.

Periodic Status Briefs. The PMO sponsored status reviews where the various DoD Component PKI offices provided status updates on their PKI programs. The PMO developed a report template to facilitate status reporting during the reviews. The PMO used the template as a status-tracking tool to assess time-based performance relating to the DoD PKI Implementation Plan. Results were compared to a predetermined goal to measure progress. Additionally, the PMO published a monthly PKI electronic letter that provided a source of information for DoD Component PKI offices on PKI and PMO activities. The PMO also provided quarterly PKI status reviews to the DoD CIO.

Unfunded Requirements. Through discussions with the PKI working groups, the PMO identified several unfunded requirements for the DoD PKI Program and briefed those requirements to the DoD CIO during periodic meetings. The unfunded requirements included operating PKI in a tactical environment, enabling applications to work with the PKI, security support for the Common Access Card (CAC), and middleware[8] development for CAC readers.

[8]Middleware is a layer of software between the network and applications that provides services, such as, identification, authentication, authorization, directories, and security.

PMO Management of the DoD PKI Program

The PMO had not managed the DoD PKI program as a DoD enterprise-wide IT investment, as advocated in the CCA. The PMO had not developed an IT investment plan that identified performance measures for the DoD PKI Program or adequately managed risks that could affect the PKI Program. Also, the PMO had not followed the intent of DoD acquisition policy by developing a process to document and manage cost, performance, and schedule parameters for PKI. The development of an IT investment plan and compliance with the intent of DoD acquisition policy and the CCA are discussed below.

IT Investment Management. The DoD developed an investment guide, "Department of Defense Guide for Managing Information Technology (IT) as an Investment and Measuring Performance (DoD IT Guide)," February 10, 1997, which establishes an analytical framework for linking IT investment decisions to strategic objectives, business plans, and organizational mission performance. The DoD IT Guide recommends the use of a consistent set of objective, outcome-oriented performance measures to ensure that the right things are being measured and that problems are identified as early in the process as possible. Because the DoD IT Guide links recommended IT investment policies to requirements, such as the CCA and Government Performances and Result Act requires, performance measures must be quantifiable, measurable, and comparable against an established baseline. The PMO used time-based performance measures to determine the progress that DoD Components were making in their respective PKI programs. However, those measures did not assess operational performance for the overall DoD PKI Program. Although DoD will issue Class 3 certificates to more than 3.5 million DoD military, civilian, and contractor employees, the PMO had not established operational performance measures, such as number of registration authorities required to issue certificates versus number of registration authorities available to issue certificates. Consequently, DoD will be unable to effectively assess whether the PKI Program is meeting user needs.

Risk Management Plan. When managing an IT Investment, the DoD IT Guide requires that risk assessments be performed to expose potential technical and managerial weaknesses. Specifically, risks must be assessed using a well-defined, documented process, or a risk management plan, to monitor, manage, and mitigate associated risks. The PMO identified and documented risks associated with the implementation of the PKI Program in the PKI Roadmap for DoD but did not identify the associated cost, performance, or schedule parameters and risks for the overall PKI Program. Further, the PMO had not developed a plan of action that included alternative solutions to mitigate the risks associated with PKI initiatives that are not controlled by the PMO. The cost, performance, and schedule of initiatives that are not controlled by the PMO would affect the implementation of the PKI Program. See Appendix D for a discussion on the PKI initiatives that are not controlled by the PMO.

Compliance with DoD Acquisition Requirements. DoD Instruction 5000.1, "The Defense Acquisition System," October 23, 2000, exists to secure and

sustain the nation's investments in the technologies, programs, and products necessary to achieve the National Security Strategy and to support the Armed Forces. The primary objective of Defense acquisition is to acquire quality products that meet user needs and provide measurable improvements to mission accomplishment and operational support, in a timely manner, and at a fair and reasonable price. Consequently, decision-makers and program managers are required to tailor acquisition strategies that:

- are consistent with common sense;
- conform to sound business management practices,
- comply with applicable laws, defense policies and regulations; and
- address the time-sensitive nature of the user's requirements to fit the particular program.

As of August 2001, the PMO had not documented compliance with the intent of DoD acquisition policy. DoD considers IT investments, such as the PKI Program, to be special interest initiatives that are not subject to normal DoD acquisition policy requirements. However, sound business practices and an investment of $712 million for the PKI Program dictate a need for a process to assess progress towards established goals, especially for cost, performance, and schedule. Establishing parameters that define minimum acceptable value and maximum allowable value would allow DoD to evaluate investments, such as the PKI Program.

Compliance With the Clinger-Cohen Act (CCA). The CCA, which is addressed in the DoD IT Guide, provides statutory requirements for managing IT investments within the Federal Government. The CCA requires agencies to design and implement a process to maximize the value and assess and manage the risks of IT acquisitions. Further, the CCA requires agencies to devise a process to obtain timely information on the progress of an investment in an information system, including milestones for measuring that progress, on an independently verifiable basis, in terms of cost, capability of meeting specified requirements, timeliness, and quality.

As of August 2001, the PMO had not documented the compliance of the PKI Program with the DoD implementation of the CCA. Specifically, the PMO, in conjunction with the office of the DoD CIO, had not:

- Designed a process for maximizing the value and managing the risk of PKI;
- Prescribed performance measures that will show how well the PKI capability will support agency programs and mission requirements; and

- Provided the means for external management to obtain timely information regarding PKI progress that included a system of milestones for measuring progress on a independently verifiable basis in terms of cost, timeliness, quality, and capabilities versus requirements.

Chief Information Officer Oversight and Management for the DoD PKI Program

Congress enacted reform legislation to improve the methods by which Federal agencies select and manage IT resources. Those IT investments must provide measurable improvements in mission performance. To comply with congressional requirements, the Secretary of Defense delegated responsibility to the DoD CIO to provide oversight and management for all DoD IT investments.

As of August 2001, the office of the DoD CIO had not provided oversight or advised the PKI PMO on acquisition requirements for the PKI Program, which was designated as a special interest initiative. The Deputy CIO memorandum, "Designation of Major Automated Information System Acquisition Programs/ Special Interest Initiatives and Related Oversight Requirements," May 5, 1999, provided general guidance for programs designated as special interest initiatives. Specifically, the memorandum required CIO personnel to:

- incorporate into regulatory guidance and oversight processes those requirements included in the CCA for IT investments; and to
- tailor management, oversight, and quarterly reporting requirements to ensure that warfighter requirements are met.

However, CIO personnel did not follow that guidance and did not establish or tailor management, oversight, or reporting requirements for the PKI Program, as specified by the May 1999 memorandum. Specifically, DoD CIO oversight officials did not require the PMO to:

- submit an acquisition strategy for review and approval;
- coordinate and obtain consensus on acquisition requirements that added value to the PKI Program, especially for cost, performance, and schedule; and
- develop or submit acquisition milestone exit criteria, such as an information assurance strategy, analysis of alternative, or economic analysis.

On March 30, 2001, the CIO updated the May 5, 1999, memorandum to identify those DoD information systems designated as major automated information systems subject to the requirements outlined in the Defense Acquisition System guidance. However, the March 2001 memorandum did not address oversight requirements for special interest initiatives. Instead, the

March 2001 memorandum stated that the CIO would issue separate guidance on major IT investments subject to CIO management oversight by the end of FY 2001. The memorandum also stated that the CIO would continue to oversee special interest initiatives that were under active oversight, where the CIO office reviewed acquisition documents, exit criteria, or evaluated the progress of the program. However, because the PKI Program was not under active acquisition oversight, the CIO did not have an effective means to minimize the risk for the DoD-wide IT investment or to ensure its compliance with defense acquisition and CCA requirements. The CIO must oversee the performance of IT programs, including the PKI Program, to evaluate the performance of those programs on the basis of the applicable performance measurements, and advise DoD management on whether to continue, modify, or terminate a program or project.

Conclusion

The DoD PKI Program is an evolving program, which is dependent upon technological advancements and commercial products. Coordinated management and oversight are essential to the successful implementation of this DoD-wide investment. Although the PMO addressed the changing requirements of the PKI Program, additional challenges remain. The PMO needs to address cost, performance, and schedule parameters of and risks to PKI implementation and develop a plan of action that includes solutions to mitigate risks associated with PKI initiatives that are not controlled by the PMO. Otherwise, DoD will not be able to adequately assess cost, performance, and schedule risks to PKI Program implementation and use those assessments to determine whether the PKI Program is cost-effectively meeting security requirements and user needs.

Recommendations and Management Comments

1. We recommend that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) develop and implement oversight and management criteria for the DoD Public Key Infrastructure investment in accordance with DoD Directive 5000.1, "The Defense Acquisition System."

2. We recommend that the Director, DoD Public Key Infrastructure Program Management Office, review the "Department of Defense Guide for Managing Information Technology as an Investment and Measuring

Performance," February 10, 1997, and develop an Information Technology Investment Management Plan for the DoD Public Key Infrastructure that addresses, at a minimum:

a. Performance measures that show how the Public Key Infrastructure capability will support agency programs and mission requirements;

b. A risk management plan that identifies cost, performance, and schedule parameters and risks for the overall Public Key Infrastructure Program; and provides alternative solutions to mitigate risks associated with Public Key initiatives that are not controlled by the Program Management Office; and

c. Application of DoD acquisition policy requirements to the DoD Public Key Infrastructure Program, to include cost, performance, and schedule parameters.

Management Comments

The Director, Information Assurance, provided a consolidated response for the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) and the Director, DoD Public Key Infrastructure Program Management Office. Both offices fully concurred with the report finding and recommendations.

The Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) also stated that a recommendation was made to designate the Public Key Infrastructure Program as a Major Automated Information System on November 7, 2001, with the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) as the Milestone Decision Authority. Also, the acquisition process will be tailored, to the extent feasible, to take into account program maturity to enable speed and flexibility in program implementation.

Appendix A. Audit Process

Scope

Work Performed. We reviewed and evaluated guidance for the DoD PKI Program contained in policy memorandums, "DoD Public Key Infrastructure," May 6, 1999 (canceled) and August 12, 2000; "Smart Card Adoption and Implementation," November 10, 1999; and "PKI Operating Documents," December 13, 1999. We also reviewed requirements for the CCA and DoD acquisition policy.

We visited the DoD PKI Program Management Office to evaluate the management and implementation of the PKI program within DoD. We also visited the Services' PKI program management offices to gain an understanding of the component-level and associated PKI beta tests to assess the status, progress, and implementation of the PKI programs.

General Accounting Office High-Risk Area. The General Accounting Office lists information assurance as a high-risk area.

Methodology

Audit Type, Dates, and Standards. We performed this economy and efficiency audit from October 2000 through August 2001 in accordance with generally accepted government auditing standards. We did not use computer-processed data for this audit.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available on request.

Management Control Program Review

We did not review the management control program related to the overall objective because DoD designated information assurance as a systemic management control weakness in the FY 2000 Annual Statement of Assurance.

Prior Coverage

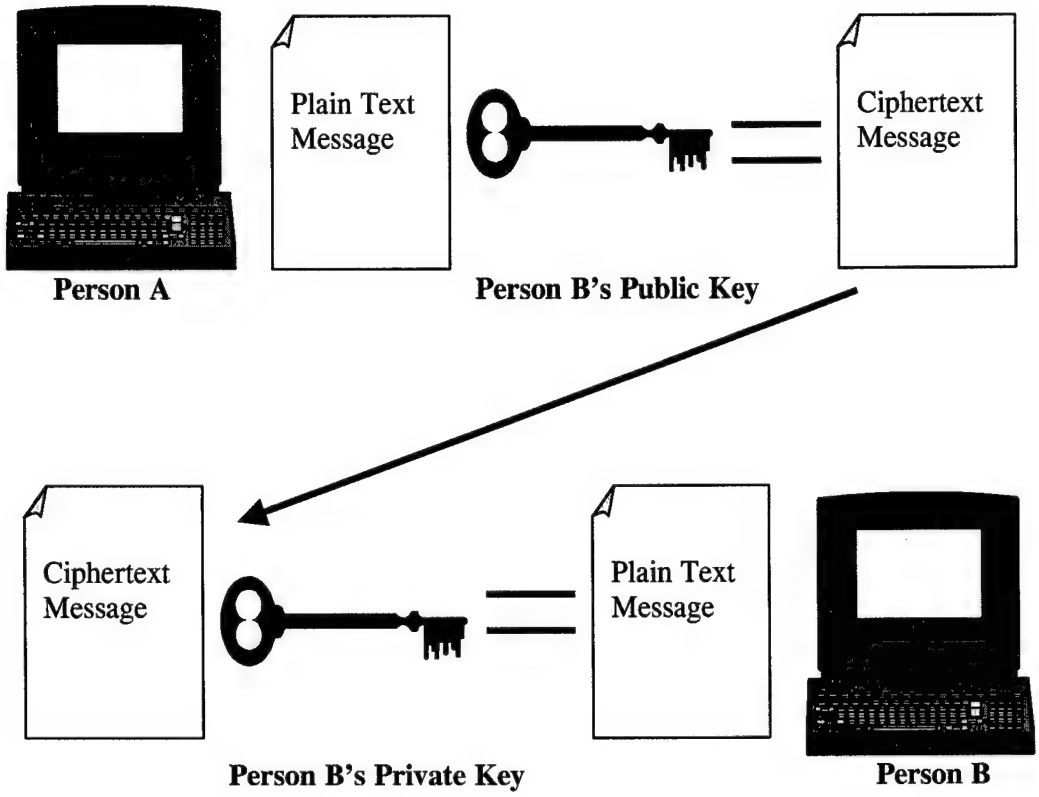
The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to information assurance issues. General Accounting Office reports can be accessed over the Internet at http://www.gao.gov. Inspector General, DoD, reports can be accessed at http://www.dodig.osd.mil.

General Accounting Office

General Accounting Office Report No. 01-277, "Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology," February 2001

General Accounting Office Report No. NSIAD-00-108, "Defense Management: Electronic Commerce Implementation Strategy Can Be Improved," July 2000

Appendix B. Public Key Encryption



Person A writes a plain text message and encrypts it using person B's public key. Then Person A transmits the cipher text message to Person B. Person B decrypts the cipher text message using the private key. The figure represents an example of how the key pairs can work.

Appendix C. Policy Memorandums Affecting the DoD Public Key Infrastructure Program

May 6, 1999, Policy Memorandum. In Deputy Secretary of Defense policy memorandum, "Department of Defense (DoD) Public Key Infrastructure (PKI)," May 6, 1999, (superceded by policy memorandum, August 12, 2000), the Deputy Secretary directed that DoD take an aggressive approach in acquiring and using a PKI that met requirements for all IA services. The policy memorandum provided initial guidance, policy, and milestones for a common, integrated DoD PKI. The Deputy Secretary also encouraged the widespread use of PKE applications and provided the following specific guidelines for applying PKI services:

- selecting appropriate PKI certificate assurance levels
- deploying PKI registration capability for FORTEZZA-based PKI (near-term solution for Class 4) and the Class 3 (formerly Medium Assurance) PKI
- evolving certificates from Class 3 to Class 4 (now Release 3 and Release 4)
- issuing identity and encryption certificates
- establishing external certificate authorities
- establishing milestones for PKI for web servers and signed email

November 10, 1999, Policy Memorandum. In Deputy Secretary of Defense policy memorandum, "Smart Card Adoption and Implementation," November 10, 1999, the Deputy Secretary directed the use smart card technology and the CAC using the DEERS/RAPIDS infrastructure. In addition, the Deputy Secretary authorized that PKI guidance be modified to incorporate and accommodate the use of the CAC. The Deputy Secretary also directed that the CAC be used as a standard DoD identification card, building access card, and PKI certificate token carrier. Further, the Deputy Secretary directed that the CAC be issued to all active duty military personnel, selected Reserve personnel, DoD civilian employees, and eligible contractor personnel. The Deputy Secretary required an initial implementation of the CAC by December 30, 2000.

December 13, 1999, Policy Memorandum. In ASD(C^3I) policy memorandum, "Public Key Infrastructure (PKI) Operating Documents," December 13, 1999, the ASD(C^3I) required the DoD PKI PMO to update the operating guidance, specifically, the DoD PKI Roadmap and the DoD X.509 Certificate Policy, to

reflect changes in program direction or strategy. The ASD(C^3I) also required the PMO to coordinate the Roadmap with final decisions concerning the CAC and the Global Information Grid programs.

August 12, 2000, Policy Memorandum. In ASD(C^3I) policy memorandum, "Department of Defense (DoD) Public Key Infrastructure (PKI)," August 12, 2000, (canceled policy memorandum dated May 6, 1999), the ASD(C^3I) updated the DoD guidelines and policies for the development and implementation of a DoD-wide PKI and aligned PKI activities and milestones with the CAC. The ASD(C^3I) also:

- mandated CAC as the primary token platform for PKI certificates;
- revised requirements for registration capability to December 2001;
- designated DEERS/RAPIDS as the primary registration platform and required the integration of DEERS/RAPIDS with the PKI capability;
- required DEERS/RAPIDS initial operational capability by December 2000; and
- required issuance of Class 3 certificates to DoD users by October 2002.

Evolution of the DoD PKI Program Based on Policy Memorandums. Based on the May 6, 1999, policy memorandum, the Deputy Secretary of Defense directed DoD to deploy registration capability based on two PKI levels:

- the FORTEZZA-based PKI (for high-level assurance) and
- the Class 3 PKI (for medium level assurance).

Both infrastructures will use software-based tokens to protect and transport private keys. Moreover, every DoD organization was required to have the capability to issue Class 3 certificates by October 2000, and required the issuance of Class 3 certificates to all DoD users by October 2001.

Based on the November 10, 1999, policy memorandum, the Deputy Secretary of Defense designated the CAC as the token for PKI because smart cards were already being used in various operational and business applications as an authentication token for certificates and as a private key for digital signature and access authentication. Consequently, the memorandum changed the requirement to protect and transport private keys from a software-based token to a hardware-based token, the CAC. In addition, the Deputy Secretary required an initial implementation of the CAC by December 30, 2000.

The August 12, 2000, policy memorandum extended the date for DoD Component registration capability from October 2000 to December 2001. Also, the date for issuance of Class 3 certificates for DoD users was changed from October 2001 to October 2002.

Appendix D. Public Key Infrastructure Initiatives That Are Not Controlled by the Program Management Office

Registration Platform for PKI. Deputy Secretary of Defense policy memorandum, "Smart Card Adoption and Implementation," November 10, 1999, directed the use of smart card technology, the CAC, and the DEERS/RAPIDS infrastructure for the PKI Program. Based on the memorandum, ASD(C^3I) designated the DEERS/RAPIDS as the primary registration platform to issue PKI certificates for Class 3 and, subsequently, Class 4 certificates, on the CAC. Additionally, the ASD(C^3I) required that all users have Class 3 certificates by October 2002. To support the CAC registration requirements, the Defense Manpower Data Center, which is the system owner, began security and technical upgrades of DEERS/RAPIDS workstations. As of June 2001, the DEERS/RAPIDS upgrades were behind schedule, potentially delaying the proposed rollout milestone date and the initiation of CAC issuance. Based on discussions with Service PKI offices, the milestone slippage threatens their ability to meet the October 2002 deadline to issue Class 3 certificates on the CAC. However, a plan of action providing alternatives, such as issuing software tokens until the registration workstations are ready or issuing tokens based on validated need, could provide temporary solutions for DoD if DEERS/RAPIDS is not ready.

Public Key-Enabled (PKE) Applications Progress. For the PKI to operate, DoD has to prepare, or enable, applications to work with the infrastructure. Otherwise, DoD could have an expensive infrastructure that has no practical use. A PKE application can accept or process certificates to support functions, such as a digital signatures or data encryption, that provide security services. The PKE applications work with the PKI to access public key certificates, revocation information, and general information in public directories or repositories. DoD Components are responsible for paying costs associated with enabling applications for PKI because the PKE costs are not included in the $712 million budgeted for PKI. Although the PMO is not responsible for enabling applications, the PMO is developing the tools and capabilities that will be used to support the enabling of applications. A plan of action that addressed PKE application issues and shared lessons learned on applications could help DoD Components understand PKI policies, use, and interfaces and could help minimize interoperability problems that could result from enabling applications.

Middleware and Card Reader Requirements. The DoD PKI will use card readers to download information from hardware tokens (the CACs). Middleware enables the readers and the tokens to communicate with the computer software. The Smart Card Senior Coordination Group developed technical specifications for middleware and card readers, and a number of vendors have met those specifications. Because DoD Components will be responsible for purchasing their own card readers and middleware, it is unlikely

that all Components would purchase the same type of card reader. Consequently, the use of different card readers could result in incompatibility among the multiple card reader systems. Additionally, different operating systems require different middleware, further increasing the chance of incompatibility. The PMO realized that complete compatibility between all card readers and middleware within the DoD would not be possible. However, the PMO had not devised a plan for minimizing incompatibility and maximizing use of middleware and card readers among DoD Components, such as evaluating readers and developing a list of vendors that provide compatible card readers.

Directories. Directories are used as a repository for the distribution of the certificates and certificate revocation lists. Specifically, directories will be used to identify and authenticate certificates of users and entities. The Defense Information Systems Agency will establish the Global Directory Services to meet this requirement. Although the directories were scheduled to be fully operational by December 2004, the PKI PMO office will work with the Defense Information Systems Agency to activate the PKI function of the directories earlier than that date. However, the control of the directories is external to the PMO and must be considered as an increased external risk that could affect the successful implementation of the DoD PKI Program. Because of the increased risk, the PMO may need to identify an alternate plan of action to identify and authenticate certificates if the directory function is not available prior to PKI implementation.

Common Access Card Security Requirements. The X.509 Certificate Policy, December 13, 1999, identified the technical specifications and security capabilities necessary for the hardware token for the CAC. The National Institute of Standards and Technology published a list of compliant cryptographic modules that met the minimum requirements defined in the Certificate Policy. Both the DoD Certificate Policy and the National Institute of Standards and Technology identified vendors that produced compliant cryptographic modules; however, the Navy selected a CAC that did not meet the established technical and security requirements of the Certificate Policy and National Institute of Standards and Technology. According to the PKI PMO, the Navy chose the CAC because the functions that DoD Components required were not available with the other CACs. Although the PMO stated that the CAC should be compliant by July 2001, the PMO had not developed a plan showing an alternate course of action if the CAC did not meet security requirements within the planned milestone.

Key Recovery Policies and Procedures. The PKI concept proposed the use of encryption certificates to enable the user to encrypt and decrypt e-mail messages and files. The public key of the certificate will be used to encrypt the data and the private key will be used to decrypt the data (or vice versa). If the private key is unattainable due to loss, termination, or theft, the encrypted data cannot be decrypted, which could lead to information loss. To mitigate information loss, DoD needs a comprehensive key recovery policy that addresses the threat, risk, and vulnerabilities of private key loss. The policy should also provide

technical solutions for recovery of DoD encrypted information, or an alternate plan of action that addresses information loss because of loss, theft, or unavailability of keys.

Unfunded Requirements. The PMO had not developed a plan to address DoD PKI Program requirements that could affect the successful implementation of the PKI program. Specifically, the DoD Components identified requirements that were not included in their budgets for FYs 2002-2005 but the requirements were needed for the PKI. Unfunded requirements included:

- Two levels of assurance operating concurrently (Class 3 and Class 4)*. Although Class 4 will replace Class 3, DoD will have an overlap of Class 3 and Class 4 with the associated costs.
- PKE applications. Although PKE applications are required for PKI, DoD Components must enable applications at their own cost. The amount budgeted for PKI is for infrastructure only.
- Security support for the CAC. Although the CAC is the designated token for certificates for DoD, costs for security support requirements associated with the CAC have not been funded.
- Middleware. The middleware and card readers are needed to work with the CAC. DoD Components must pay for their own middleware and card readers.
- PKI operation in a tactical environment. To support the warfighter, PKI must be portable. Costs associated with a portable PKI have not been funded.

The PMO briefed the unfunded requirements to the DoD CIO. However, a plan of action identifying the costs of the unfunded requirements, showing the overall effect that the funding shortfalls could have on the DoD PKI Program, and suggesting alternate solutions to address the funding shortfalls is needed for the PKI Program.

* Upon the completion of testing, Class 3 and Class 4 will be renamed Release 3 and Release 4. For purposes of this report, we are using their current naming conventions.

Appendix E. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller/Chief Financial Officer)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
  Director, Program Analysis and Evaluation
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Assistant Secretary of Defense, Deputy Chief Information Officer
  Deputy Assistant Secretary of Defense, Security and Information Operations
    Director, Infrastructure and Information Assurance
      Director, Defense-Wide Information Assurance Program
      Director, Public Key Infrastructure Program Management Office

Joint Staff

Director, Joint Staff
  Chief Information Officer, Joint Staff

Department of the Army

Director of Information Systems for Command, Control, Communications and Computers
Chief Information Officer, Department of the Army
Auditor General, Department of the Army

Department of the Navy

Director, Space, Information Warfare, Command and Control
Director, Command, Control, Communications, and Computers, Marine Corps
  Director, Marine Corps Network Operations Center
Commander, Marine Corps Systems Command
Chief Information Officer, Department of the Navy
Auditor General, Department of the Navy
Naval Inspector General
Inspector General, Marine Corps

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Deputy Chief of Staff, Communications and Information
Commander, Air Force Materiel Command
  Commander, Cryptologic Systems Group, Electronic Systems Center
Chief Information Officer, Department of the Air Force
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Information Systems Agency
  Chief Information Officer, Defense Information Systems Agency
Director, National Security Agency
  Inspector General, National Security Agency

Non-Defense Federal Organizations

Office of Management and Budget
  Office of Information and Regulatory Affairs

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology and Procurement Policy, Committee on Government Reform

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

November 9, 2001

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Audit Report on the Implementation of DoD Public Key Infrastructure Policy and Procedures (Project No. D2001AS-0008)

This is a consolidated response from OASD(C3I) and the DoD Public Key Infrastructure Program Management Office (PKI PMO) to the subject Inspector General, DoD, audit report. The OASD(C3I) and the PKI PMO have been working closely together over the summer to address many of the same concerns raised in the subject report and generally share a common position on the issues. Thus, we feel a single unified response is appropriate.

The OASD(C3I) and the DOD PKI PMO fully concur with the report findings and the recommendations. Specifically, OASD(C3I) and the DoD PKI PMO concur that:

- OASD(C3I) develop and implement oversight and management criteria for the DoD PKI investment in accordance with DoD Directive 5000.1, "The Defense Acquisition System."

- Director, PKI PMO review the "Department of Defense Guide for Managing Information Technology as an Investment and Measuring Performance," February 10, 1997 (DoD IT Guide), and develop an Information Technology Investment Management Plan for the DoD Public Key Infrastructure program that addresses, at a minimum: Performance measures, a comprehensive risk management plan, and application of DoD acquisition policy requirements.

A recommendation was made to the ASD(C3I) on November 7, 2001 to designate the PKI program as a MAIS ACAT 1AM program, with ASD(C3I) as the Milestone Decision Authority (MDA). Several factors led to this recommendation, including the following:

- PKI, a $700 million-plus program, greatly exceeds the dollar threshold for a MAIS in DoD instruction 5000.2, and otherwise meets the definition of a MAIS.

- Since PKI is a Department-wide program and a vital element of the Department's Defense-in-Depth strategy, a more structured management and oversight framework commensurate with a MAIS is warranted.

Final Report
Reference

- Key information (e.g. performance metrics, risk management plan, compliance with DoD acquisition requirements) that is required under the Clinger-Cohen Act (CCA) and/or the DoD 5000 series and is needed to properly manage the program has not been developed.

- The OASD(C3I) Program and Evaluation office performed a "Quick Look" evaluation of PKI focusing on CCA and MAIS requirements and recommended that PKI should be immediately designated as a MAIS with the associated reporting requirements and oversight.

- The content of subject IG report which echoes much of the above.

- The DoD General Counsel office rendered an opinion that PKI should be a MAIS.

An OSD Overarching Integrated Product Team (OIPT) will be formed promptly after ASD(C3I)'s designation of PKI as a MAIS. The acquisition process for the PKI program will be tailored, to the extent feasible, to take into account program maturity to enable speed and flexibility in program implementation. The OIPT will provide acquisition oversight supplemented by day-to-day guidance provided by the NSA Senior Acquisition Executive (SAE).

The PKI PMO is generating a detailed plan for addressing PKI technology investment planning. The PKI PMO will communicate progress on the plan in a timely fashion to the IG office to ensure that the structure and plan for the effort is targeted to adequately address the issues identified in the IG report that focus directly on PMO responsibilities.

At a minimum, the IG can expect timelines will be established to ensure that performance metrics, a comprehensive risk management approach, and attention to CCA requirements are attended to. The IG will be kept informed as progress is made in these areas and other areas as identified by the OIPT as needing improvement.

My PKI point of contact is Mr. Eric Moos at 703-614-2196, or Eric.Moos@osd.mil.

Robert F. Lentz
Director, Information Assurance

cc: PKI Program Manager
DCIO

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector General, DoD, who contributed to the report are listed below.

Mary L. Ugone
Wanda A. Scott
Dianna J. Pearson
Donna Roberts
Richard B. Vasquez
Cristina Maria H. Giusti
Timothy A. Cole
Jamal E. Hall
Pamela Newkirk
Jacqueline Pugh